**STATEMENT**
**OF**
**MICHAEL JOHNSON**
**CHIEF INFORMATION OFFICER**
**U.S. DEPARTMENT OF ENERGY**

**BEFORE THE**

**SUBCOMMITTEES ON INFORMATION TECHNOLOGY**
**AND GOVERNMENT OPERATIONS**
**COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM**
**UNITED STATES HOUSE OF REPRESENTATIVES**

**May 18, 2016**

## Introduction

Good afternoon, Chairman Hurd, Ranking Member Kelly, Chairman Meadows, Ranking Member Connolly, and distinguished Members of the Committee. On behalf of the Department of Energy (DOE), I thank you for the opportunity to appear before you to discuss the Department's implementation of the *Issa-Connolly Federal Information Technology Acquisition Reform Act* (FITARA), and thank you for your efforts in ensuring that this critical law is implemented successfully. DOE welcomes the authority that FITARA provides to accomplish greater transparency and fiscal accountability over its Information Technology (IT) and cyber investments.

During my tenure at DOE, I have been working to implement FITARA and cybersecurity best practices across numerous and diverse DOE components. This work has enabled the development of strategic partnerships among departmental Program Offices and senior leaders that will allow DOE FITARA implementation to strengthen key reform initiatives, including PortfolioStat, TechStat, CyberStat, and data center optimization.

## The DOE Enterprise

I joined DOE a little over a year ago to develop and implement an effective, efficient, and inclusive cyber strategy for the DOE enterprise. The enterprise comprises 97 entities—spread across 27 states—divided among 10 Program Offices, 19 Staff Offices, 4 Power Marketing Administrations, 19 Field Sites, 17 National Laboratories, and 4 Technology Centers—each uniquely structured to perform our distinct mission. This mission spans an incredibly diverse range of portfolios from nuclear security, open science research, power administration, to environmental management.

Of the 17 National Laboratories, all but one are government-owned, contractor-operated facilities, managed through Management and Operating (M&O) contracts. The IT portion of DOE's overall budget is approximately $1.7B ($1.1B of which is spent through M&O contracts). At DOE, IT is often an integrated component of much larger non-IT investments.

The DOE enterprise is a critical factor relevant to FITARA implementation. Wherever possible, DOE leverages its existing management and acquisition processes, including National Nuclear Security Administration (NNSA). DOE's efforts to implement FITARA reflect the input of stakeholders from across the enterprise; for over a year the DOE enterprise has applied knowledge and expertise to collaboratively identify and resolve FITARA implementation issues.

## Governance

The Department's IT and cyber governance is fully inclusive, transparent, responsive, and supportive of the DOE mission. The DOE Cyber Council, chaired by the Deputy Secretary, and Information Management Governance Board (IMGB), which I chair, are our executive policy and implementation fora. The Cyber Council is chartered to, among other things, reinforce strategic and tactical information sharing and information safeguarding initiatives to ensure enterprise-wide compliance with legislative requirements, executive orders, Federal policies and rules, and Federal cybersecurity and risk management standards. The Cyber Council reviews and vets significant enterprise information resources management and cyber-related policy issues prior to a decision by the Secretary and the Deputy Secretary. The IMGB consists of senior officials from the DOE enterprise with responsibility for IT systems and cybersecurity, and serves as the forum for collaboration, development, coordination, and implementation of enterprise information resources management activities. The IMGB is structured to conduct detailed program reviews for IT investments, to include performance issues in project execution, cost, schedule, technical metrics, and risks. This supports DOE's development of accurate risk ratings for its submission to the Federal IT Dashboard. The IMGB and the Cyber Council are mature, functioning bodies, with invested and engaged stakeholders from across the DOE enterprise that meet on a regular basis.

## Budget & Acquisition

Working closely with the Department's senior leadership team, I have significant involvement in IT-based budget, procurement, and workforce decision-making. Crucial to effective DOE implementation of FITARA, is ensuring that the CIO is able to provide strategic input at the early stages of DOE's budgeting and acquisition processes. DOE is adjusting its internal budget development procedures and guidance to ensure CIO involvement in all necessary phases of its annual and multi-year planning, programming, budgeting, and decision-making. Further, DOE is working to reengineer current acquisition strategy processes to include the CIO (or representative) in all IT-related acquisition and execution decisions. The Chief Acquisition Officer (CAO), Chief Financial Officer (CFO), and I, along with DOE elements, worked collaboratively to develop an enterprise plan for the review and approval of IT acquisitions that covers acquisition plans, statements of work, and evaluation and selection criteria. The end goals are expedited final review and approval that incorporates factors such as strategic planning and sourcing, enterprise goals, licensing, and mission needs prior to spending on IT assets.

## Transparency

Greater transparency for DOE leadership into enterprise IT spending is foundational to FITARA implementation. DOE understands that improving acquisition, investment governance, and IT portfolio transparency are critical elements towards achieving mission objectives and greater savings, all while reducing cyber risk.

Data-driven decision-making is a key activity for the Department. We are currently refining the IT Portfolio reporting processes to ensure alignment with substantive processes and categories across the Department. This will provide the DOE CIO, DOE Element CIOs, and the broader DOE enterprise transparency into the enterprise IT spend across both mission and support IT, and in both major and non-major investments. Based on this, we are developing additional improvements to increase the transparency of our IT portfolio on the Federal IT Dashboard.

## Workforce & Organization

With strong leadership endorsement, the Chief Human Capital Officer (CHCO) and I are working together to develop and implement the DOE Cyber Workforce Strategy, that will define and implement a process to increase the CIO's involvement in DOE's human capital selection practices, develop performance goals with results-driven critical elements for identified positions, and enhance recruitment and retention of vital IT personnel. Our goal is to ensure that DOE's information management and cyber workforce is both well-trained and equipped to respond rapidly to evolving mission needs. We are simplifying and expediting the hiring process, and are examining workforce requirements to develop rules and practices that will sustain this critical workforce.

In accordance with Office of Management and Budget (OMB) policy, DOE is requiring all program and project managers assigned to major acquisitions to obtain the necessary certifications that meet government-wide standards for knowledge, skill, and experience. This includes mandatory training in the areas of Advanced Risk Management, Program Management and Portfolio Analysis, Agile Methodologies, and Advanced Earned Value Management Techniques. In 2015, DOE implemented a program to increase the number of Level 1, 2, and 3, Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) across the enterprise. The DOE FAC-P/PM is one step toward increasing certifications on all levels. All Elements must report project management qualifications and ensure that project managers are equipped to successfully manage major IT investments, ensuring compliance with both external and internal regulations and guidance. On a quarterly basis, DOE CIO reviews all major IT investments to ensure that the project managers assigned to those investments are FAC-P/PM certified at the appropriate level.

## Data Center Optimization

Data Center Optimization and Consolidation is central to DOE's strategy to increase effectiveness across the enterprise, reduce IT and energy costs and gain efficiencies, and reduce cyber risk associated with legacy systems. We have proactively taken steps to capture a broader enterprise-wide inventory of data centers, expanding our previous reporting by including the

breadth of our enterprise, noting that several of our mission-specific data centers are not suitable for consolidation because of the nature of their respective mission requirement, to include data processing and storage needs.

DOE continues optimization of its data centers through advanced metering and facility upgrades to improve power utilization effectiveness. DOE will continue to refine its data center optimization initiative strategy, modernize its IT infrastructure, migrate workloads to the Cloud, and optimize its data centers for greater operational and energy efficiency. To that end, DOE established an enterprise-wide Data Center Working Group, chartered to identify best practices in data center metering, optimization, consolidation, and cloud migration.

From 2010 to present, DOE reported a total of 217 enterprise computing data centers. During this timeframe, 75 data centers have been closed, leaving a total of 142 open enterprise data centers. The closures have resulted in a savings to the Department of just over $17M.

## Cybersecurity

The DOE approach to cybersecurity addresses dynamic and evolving cyber threats. To achieve our cyber security mission objectives, we consolidated cyber initiatives into a unified and prioritized DOE plan that collects them into several areas including: (1) Information Resources Management best practices (to improve effectiveness, reliability, and efficiency); (2) modernization (to move quickly from legacy to transformative solutions); (3) strengthened cybersecurity fundamentals (to reduce risk and defense-in-depth capabilities); and (4) seamless integration of Information Resources Management operations and cyber defense (to combine situational awareness of threat, operational status and events, and cyber incidents).

DOE has made significant contributions to the real-time dissemination of actionable cyber threat information, both inside and outside the Department. Our intent is to leverage the full complement of enterprise capabilities and protect the DOE enterprise.

## Conclusion

DOE is committed to greater transparency and fiscal accountability over its IT and cyber investments. The Department is actively working to implement FITARA in a manner that is best-suited to the structure and functioning of DOE's complex enterprise. Through a department-wide inclusive, and collaborative process, we have made major strides towards that goal, although further work is needed. Your interest and support are vital to our success. It has been my honor to provide this testimony to you. I would be pleased to address any questions that you may have for me.

**Michael Johnson**
**Department of Energy, Chief Information Officer**

Mr. Michael Johnson is the Chief Information Officer (CIO) for the U.S. Department of Energy (DOE), where he leads and manages cybersecurity, cyber (information sharing and safeguarding) enterprise integration, enterprise information resources management, cyber supply chain risk management, and DOE-HQ information technology (IT) operations. This includes DOE leadership, management, and oversight serving as DOE's Senior Agency Official for Privacy, Senior Agency Official for Records Management, Senior Agency Official for Information Sharing and Safeguarding to include DOE coordination of National Security Systems, and Senior Agency Official for Spectrum Management. Mr. Johnson is the DOE representative to the White House National Security Council Cyber Response Group (CRG), the Cyber Interagency Policy Committee (IPC), the Federal CIO Council, the Federal Privacy Council, and he serves as the co-chair of the Committee on National Security Systems (CNSS).

Accountable to the Secretary and Deputy Secretary, Mr. Johnson leads Department-wide cyber efforts, including cybersecurity strategy, policy, and operations. He has instituted a cyber distributed, shared risk management framework that integrates cyber operations coordination, cyber intelligence, and cyber incident response. Mr. Johnson is leading the development of an integrated, DOE enterprise-wide automated cyber information sharing and advanced threat analytics capability to ensure real-time enterprise cyber situational awareness and incident response. DOE is advancing cyber hardening by implementing information resources management best practices and modernization initiatives, to include systematic tracking of assets, continuous software updates, and strategic technology refresh such as deploying infrastructure-as-a-service. Under Mr. Johnson's leadership, DOE is reducing cyber risk by strengthening cybersecurity fundamentals to include strong multifactor authentication, network and privileged user access segmentation, advanced continuous monitoring, and automated vulnerability identification. Recognizing that cyber research and development (R&D) is critical to outpacing our adversaries, Mr. Johnson is engaging the National Laboratories to franchise the world-class cyber R&D performed by these institutions to the benefit of the broader DOE enterprise and the U.S. interagency, to include advanced continuous monitoring, automated cyber threat analysis and risk modeling, and efficient security and privacy architectures.

Mr. Johnson has more than 25 years of management, policy, and operational experience, with deep expertise in cybersecurity, information sharing and safeguarding, intelligence, and national continuity policy. Prior to joining DOE, Mr. Johnson served as the Assistant Director for Intelligence Programs and National Security Systems in the White House Office of Science and Technology Policy. He has held positions at the Department of Homeland Security, where he served as the Chief Scientist within the Office of Intelligence and Analysis, and he was appointed the first Deputy Associate Director of National Intelligence for Information Sharing and Deputy, Intelligence Community Information Sharing Executive in the Office of the Director of National Intelligence. Previously, Mr. Johnson managed national security systems analysis, and served as senior scientist, computer engineer, and intelligence analyst at Sandia National Laboratories. Mr. Johnson has a B.S. in Computer Engineering and an M.S. in Computer Science, with specialization in parallel and distributed simulation, embedded systems, and network protocol design.